Biometrics in a Mobile World

Christoph Busch

Gjøvik University College
http://www.christoph-busch.de

Sikkerhetssymposiet

Bergen - October 28th, 2015

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Norwegian Biometrics Laboratory (NBL)

- Faculty-Members:
  - Christoph Busch
  - Patrick Bours
  - Bian Yang
  - Faouzi Alaya Cheikh
  - Sule Yildrim
  - Erik Hjelmås
  - Raghu Ramachandra
  - Katrin Franke (adjunct member)
  - Ivar Farup (adjunct member)
  - Mohammad Derawi

- PhD-Students:
  - Ctirad Sousedik
  - Edlira Martiri
  - Guoqiang Li
  - Kiran Raja
  - Martin Olsen
  - Martin Stokkenes
  - Nabeel Al-Bahbooh
  - Soumik Mondal
  - Marta Gomez (guest from UAM)

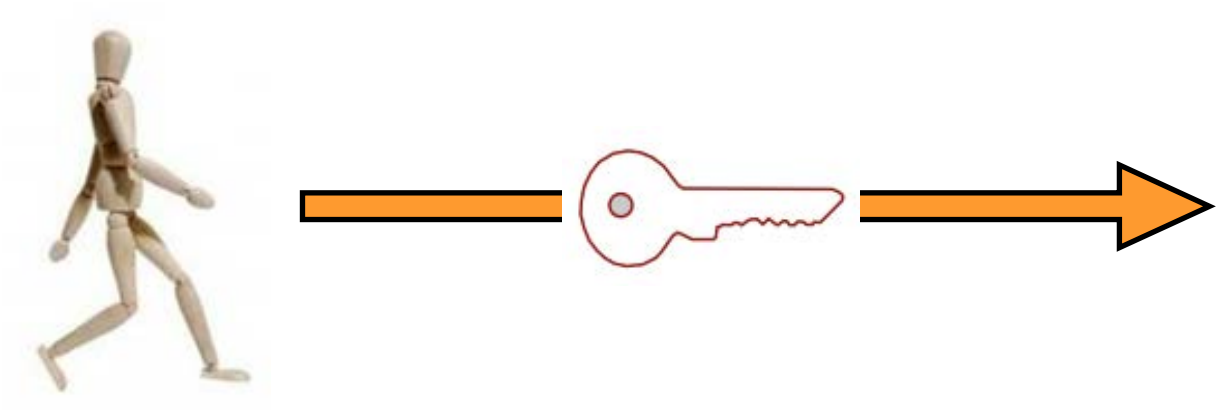
- Key-factors:
  - Since 2008, 6 EU FP7 projects,
    2 Norwegian funded project
    1 US-government funded project,
    2 research projects with the German BSI,
    4 industrial projects,
  - cooperated with > 30 research partners
  - approx 110 peer-reviewed publications

Introduction to Biometrics

Access Control

Traditionally we place between

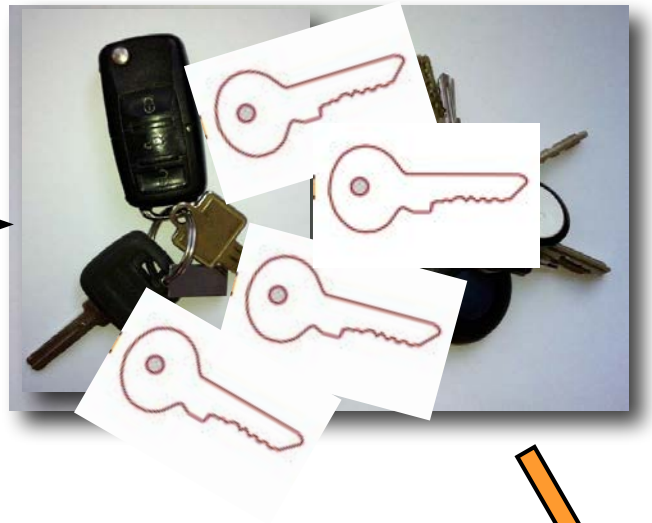
- individuals
- and objects
- a token (i.e. key)

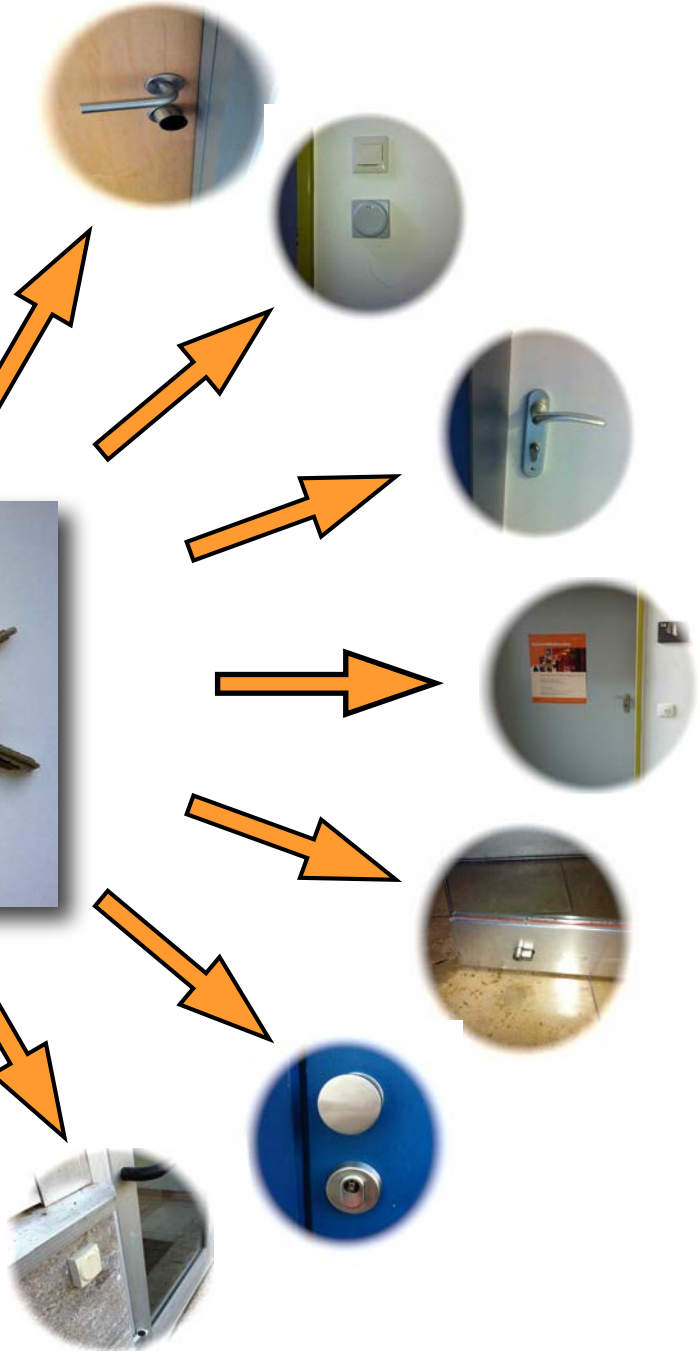


Access Control

But in reality individuals

- do not have just one
- but many keys
- granting access to many doors





Access Control

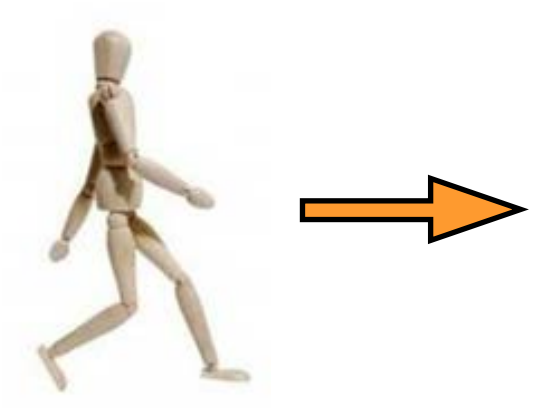
I do already have

- a Campus Card
- granting access to many doors

Access Control

For some individuals

- the collection of cards is quite impressive and inconvenient



Access Control

Identity authentication can be achieved by:

- Something you know:
  Password, PIN, other secret
- Something you own:
  SmartCard, USB-token, key
- Something you are:
  Body characteristics

Something you know or own
you may loose, forget or forward to someone else,
with biometrics this is more difficult.

- security policy not violated by delegation
- non-repudiation of transactions
  „This was initiated by *Igor Popov* misusing my card“

Security of Biometrics ?

Operators may think:

„Biometrics are not as secure as PINs“

Benchmark of Biometrics and PIN (cont.)

There are striking arguments why biometric authentication is better than the PIN

- The entropy of a 4 or 6-digit PIN is very limited
  - Even for a 6 digit numeric PIN (e.g. with the German eID card) the entropy $H = L * log_2 N$ is limited to less than 20bit (with $L=6, N=10$)
  - The reported entropy for different biometric characteristics is
    - Fingerprints 84bit [Ratha2001], Iris 249bit [Daugman2006] Face 56bit [Adler2006], Voice 127bit [Nautsch2015]

[Ratha2001] N. Ratha, J. Connell, R. Bolle: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, vol. 2091, pp. 223–228. Springer, (2001)

[Daugman2006] J. Daugman: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)

[Adler2006] A. Adler, R. Youmaran, S.Loyka: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering, (CCECE'06). pp. 210–213 (2006)

[Nautsch2015] A. Nautsch, C. Rathgeb, R. Saeidi, C. Busch: Entropy Analysis of I-Vector Feature Spaces in Duration-Sensitive Speaker Recognition, in 40th IEEE ICASSP Conference, 19-24 April 2015, Brisbane, Australia, (2015)

Introduction to Biometrics

Feature Extraction and Comparison

Analog/digital representation of the finger ridges

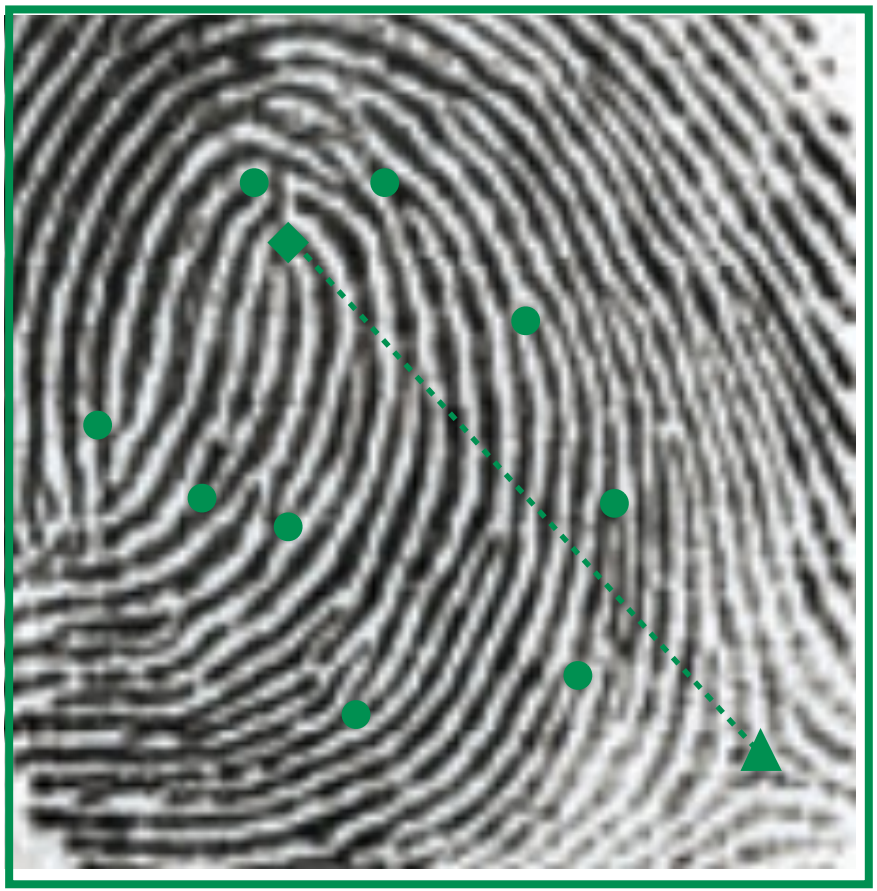
- Distinguished points of the fingerprint: Minutia

Feature Extraction and Comparison

Comparison of reference image against a probe image

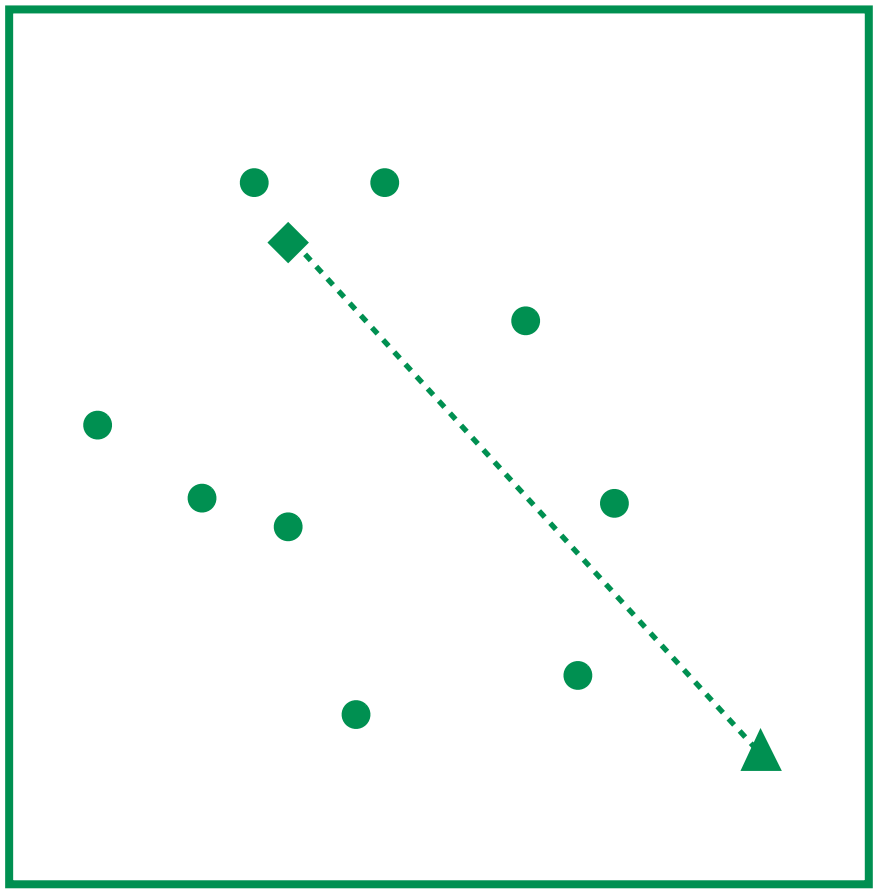
Feature Extraction and Comparison

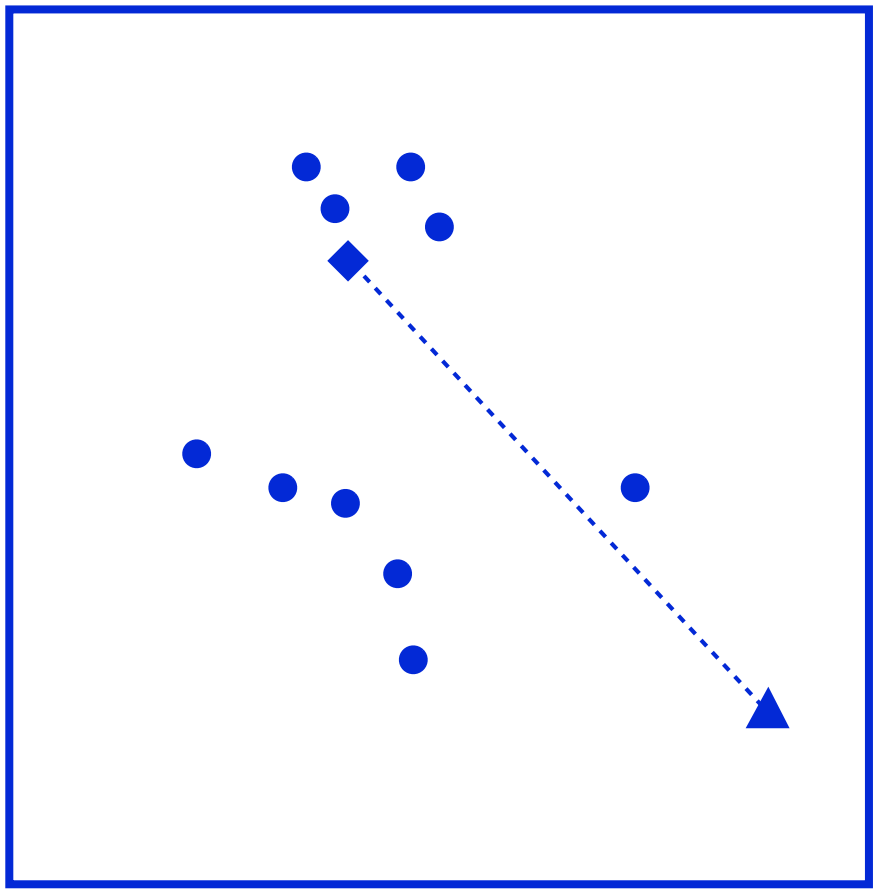
Comparison of reference image
against a probe image



Feature Extraction and Comparison

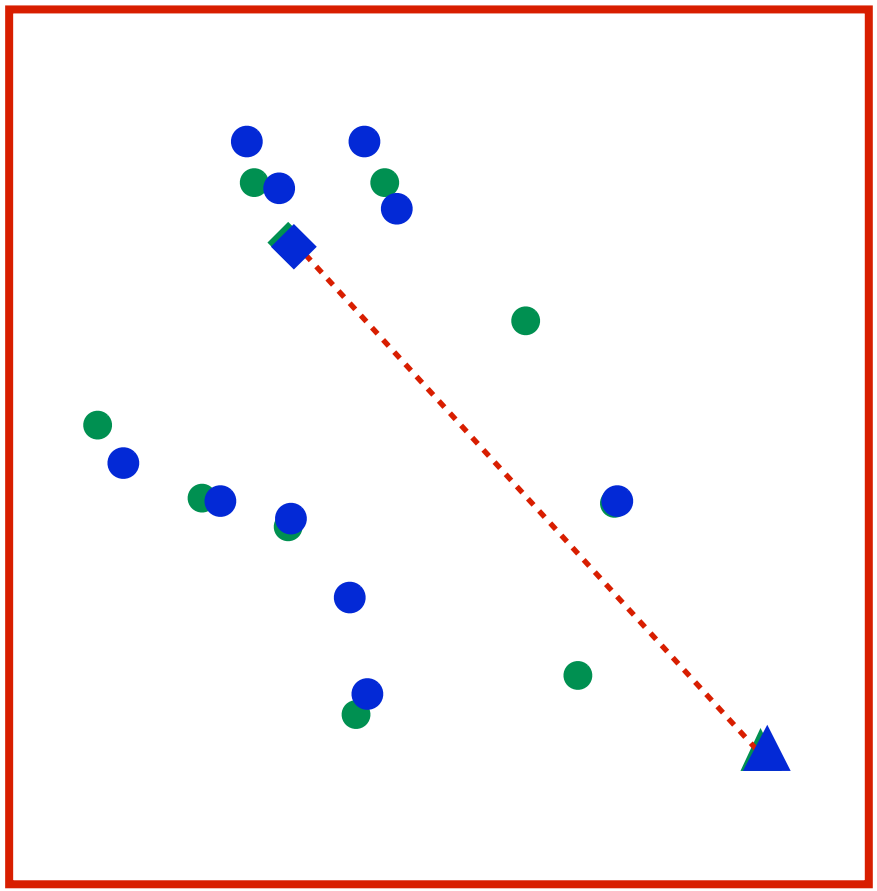
Comparison of reference feature vector against a probe feature vector





Feature Extraction and Comparison

Comparison of reference feature vector against a probe feature vector



Performance Metrics in Biometric Systems

False-Match-Rate (FMR)

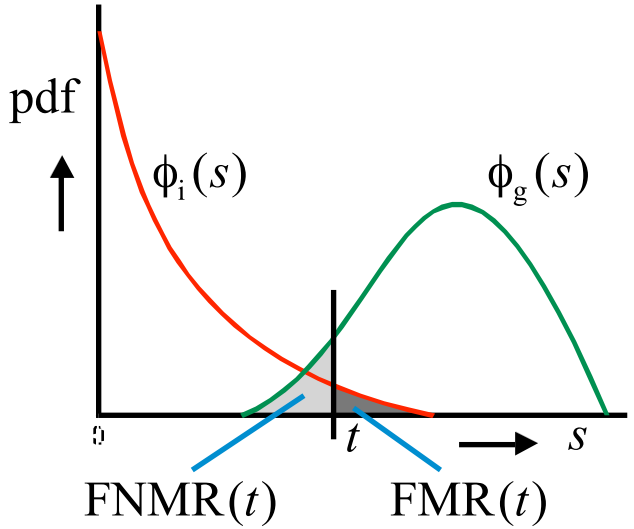
- **Def :** "*proportion of the completed biometric non-mated comparison trials that result in a false match*"
- Note: non-mated trials are also referred to as impostor trials

False-Non-Match-Rate (FNMR)

- **Def:** "*proportion of the completed biometric mated comparison trials that result in a false non-match*"
- Note: mated trials are also referred to as genuine trials

$$FMR(t) = \int_t^1 \Phi_i(s)ds$$

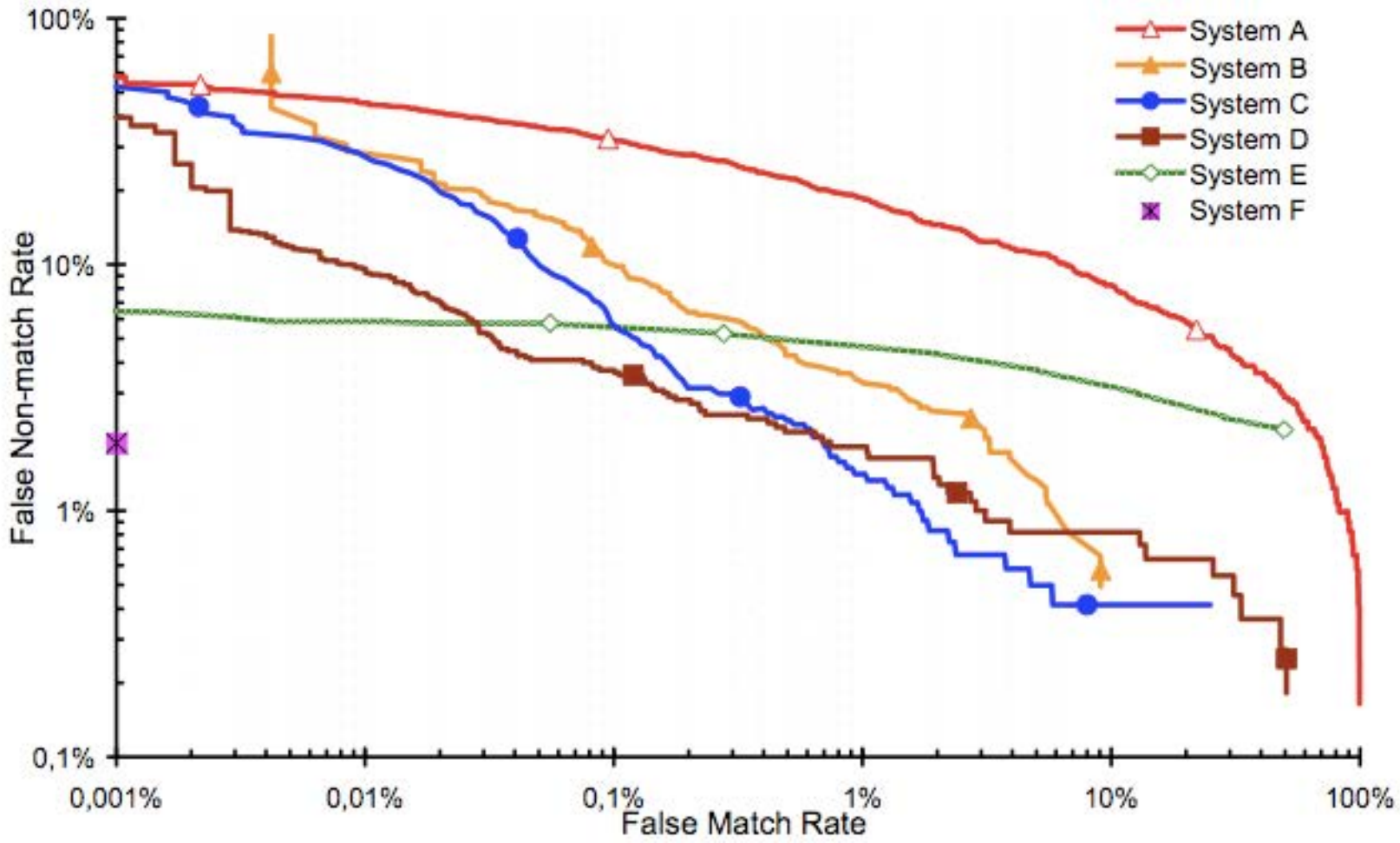
$$FNMR(t) = \int_0^t \Phi_g(s)ds$$



Graphical Presentation

DET curve (detection error trade-off curve)

- curve which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)



Biometric Applications

Biometrics and Access Control

Automated Border Control in Europe

- Automated but supervised border control since 08‘2009
- Self-Service to increase throughput

US VISIT

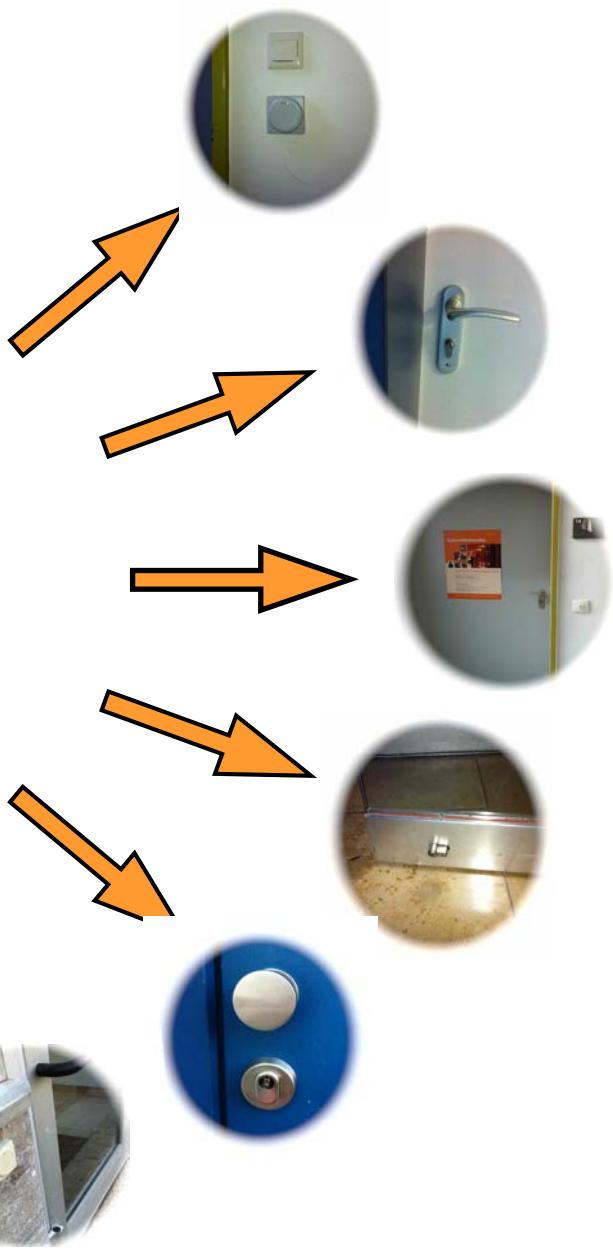
- Visitors with a criminal record are rejected

Source: US Visit

Access Control

Should we in the long term future

- have biometric access control at every door?

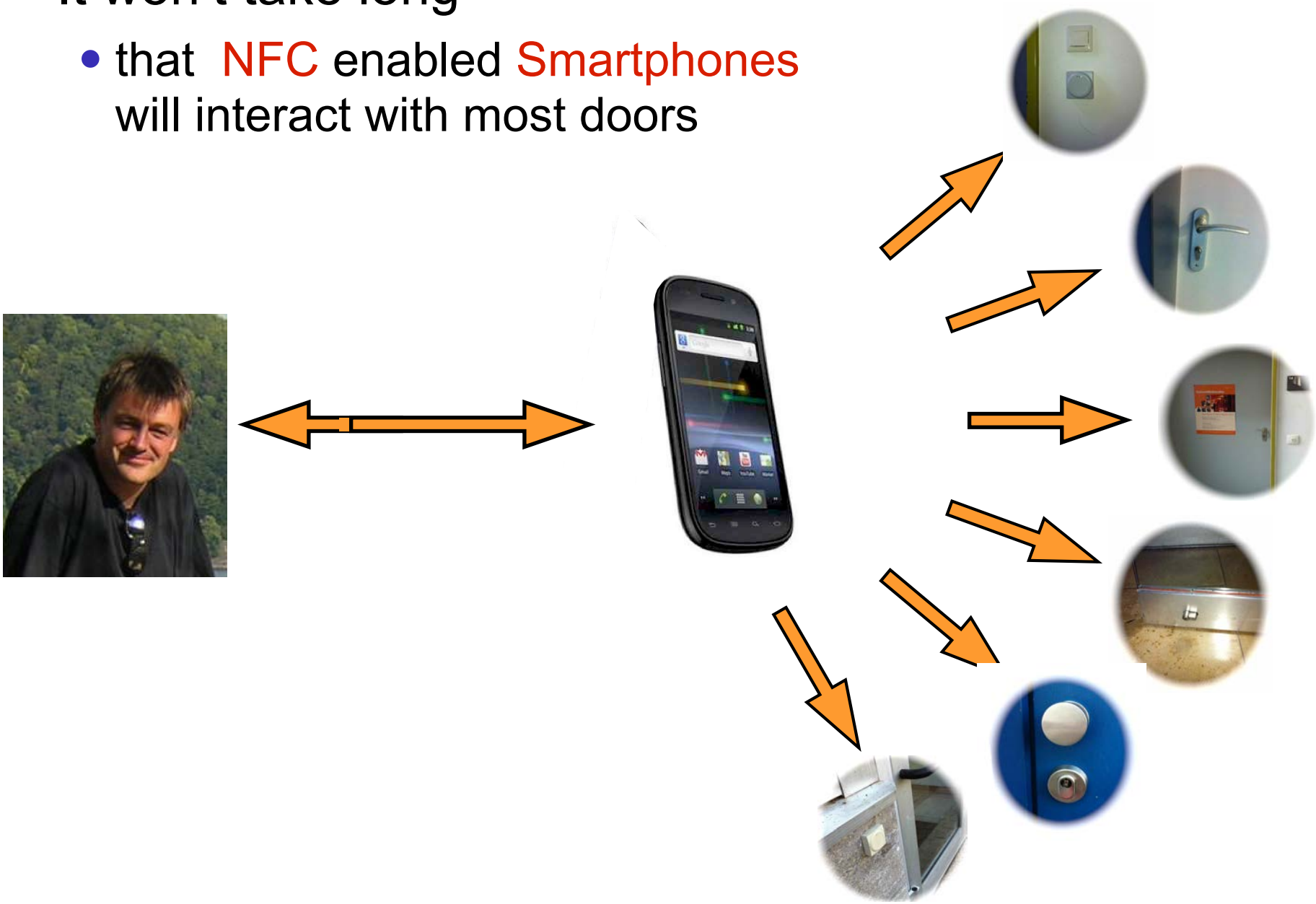


- cost factor for sensors?
- where do we store references?

Smartphone Based Access Control

It won‘t take long

- that NFC enabled Smartphones will interact with most doors



Mobile Biometrics

Smartphone Access Control

Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition
- Touchpad: allows signature recognition

Image Source: Apple 2013

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

Biometric Speaker Recognition

Offer an unobtrusive or explicit authentication method

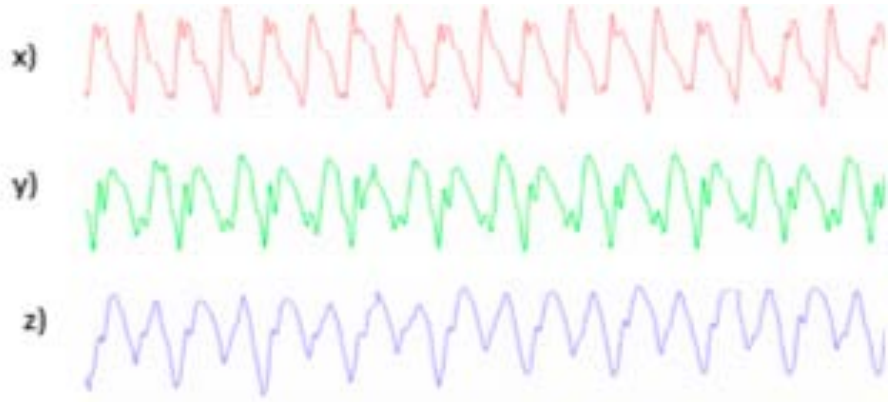
- Use embedded microphone in mobile device to record the voice signal
  - unobtrusive or
  - apply willful act for explicit transaction authorization
  - no extra hardware is needed




Biometric Gait Recognition

Offer an unobtrusive authentication method

- Use accelerometers - already embedded in mobile devices to record the gait
  - No extra hardware is necessary
  - Acceleration measured in 3-directions



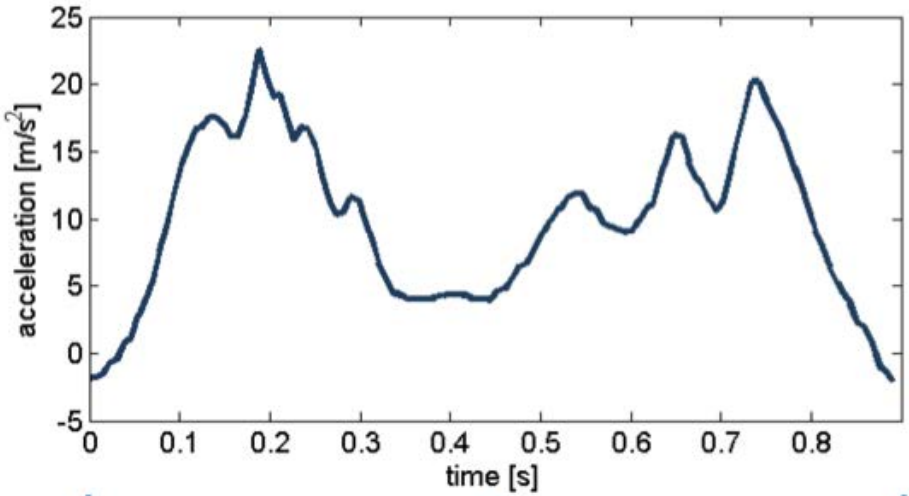
- Initial paper on this topic:

[DNBB10] M. Derawi, C. Nickel, P. Bours, C. Busch: „Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition“, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2010)

Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal



Best result

- now at 6.1% Equal-Error-Rate (EER)

Biometric Gait Recognition

- All benchmarked publications

Publication	Sensor	Sensor-position	Number Subjects	Best Result [%]
Ailisto [4], 2005	dedicated	back	36	6,4 (EER)
Rong [123], 2007	dedicated	back	21	5,6 (EER)
Pan [61], 2009	Wiimote	hip	30	70,1 (GMR)
Sprager [130], 2009	smartphone	hip	6	92,9 (CCR)
Gafurov [46], 2010	dedicated	ankle	10	59,0 (GMR)
Nickel (CASED)	smartphone	hip	48	6,1 (EER)

[NB11] C. Nickel, C. Busch „Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way they Walk“, 45th IEEE International Carnahan Conference on Security Technology (ICCST 2011)

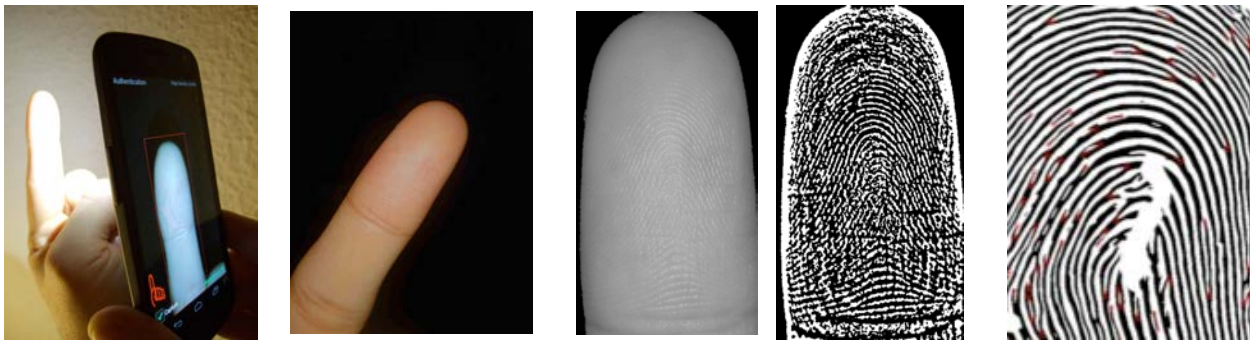
Smartphone Access Control

Capture process

- Camera operating in macro modus

Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on



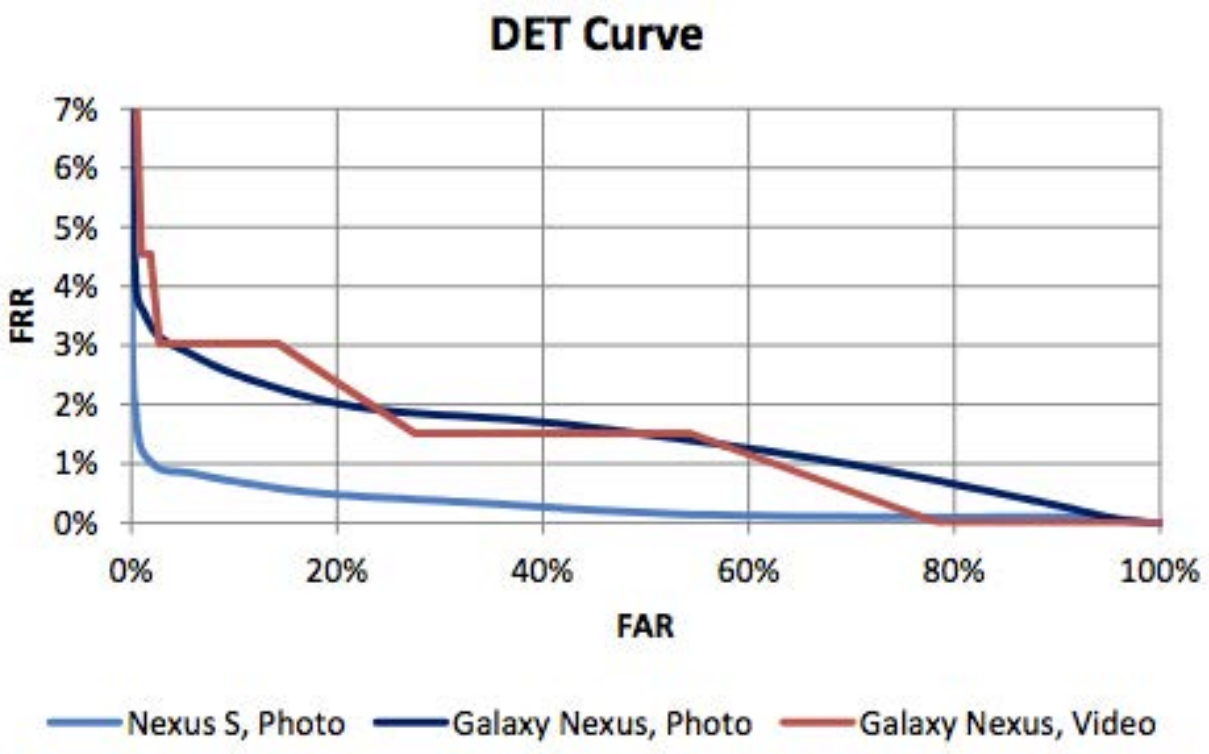
Finger illuminated

[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER



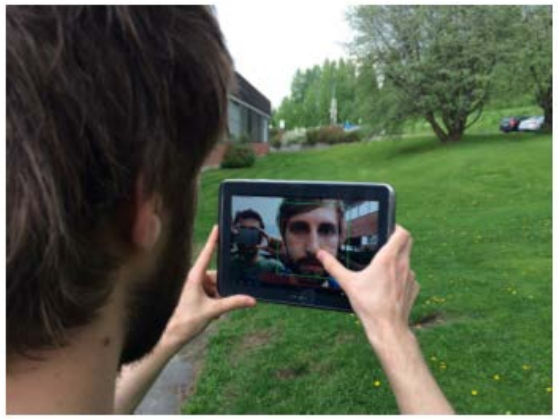
Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR=0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

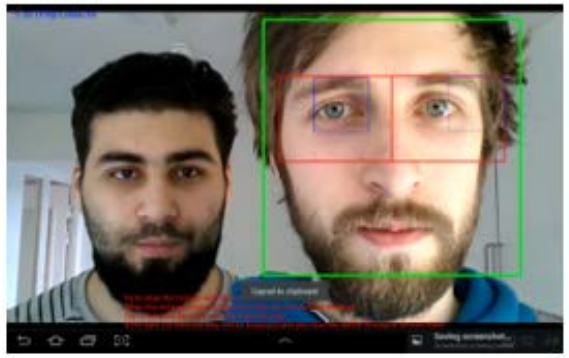
[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Biometric Eye Recognition

Images captured with either front or back camera

- Challenges
  - face and eye localization
  - feature extraction with SURF, SIFT und Binarized Statistical Image Features (BSIF)



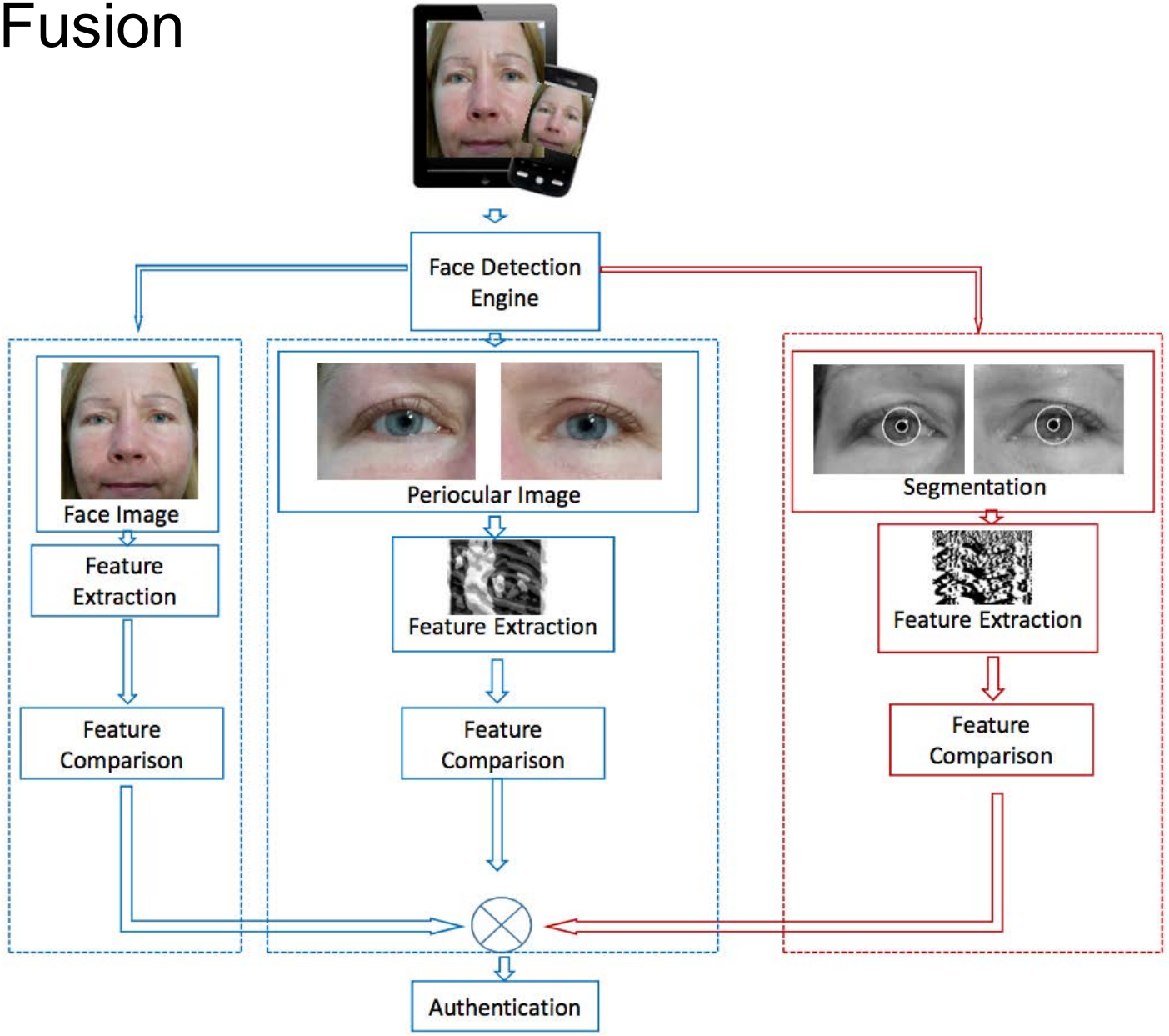


[KR12] J. Kannala and E. Rahtu. BSIF: „Binarized statistical image features“. ICPR conference, (2012)

[RRSB14] K. Raja, R. Raghavendra, Martin Stokkenes, Christoph Busch: „Smartphone Authentication System Using Periocular Biometrics“, (BIOSIG 2014)

Biometric Face and Eye Recognition

Multimodal Fusion



Biometric Face and Eye Recognition

Multimodal Fusion - Biometric Performance

Fusion Scheme	Camera	Samsung S5		Samsung Note	
		GMR@FMR=0.01%	EER	GMR@FMR=0.01%	EER
Min Rule	Back Assisted	99.17	0.43	88.57	3.43
	Back	97.12	0.93	88.13	4.34
Max Rule	Back Assisted	50.78	10.71	11.65	25.93
	Back	52.94	12.10	17.74	22.59
Product	Back Assisted	84.13	15.34	50.65	47.96
	Back	84.81	14.37	44.61	48.08
Weighted Fusion	Back Assisted	**99.13**	**0.43**	**95.52**	**2.39**
	Back	**97.98**	**0.68**	**93.52**	**2.69**

[RRB15] K. Raja, R. Raghavendra, C. Busch: " Multi-modal Authentication System for Smartphones", in Proceedings of the 8th IAPR International Conference on Biometrics (ICB), 19-22 May 2015, Phuket, Thailand, (2015)

Requirements of Operators for Mobile Biometrics

Security ?

Operators will think:

„*The biometric sensors must be robust against fake attacks*“

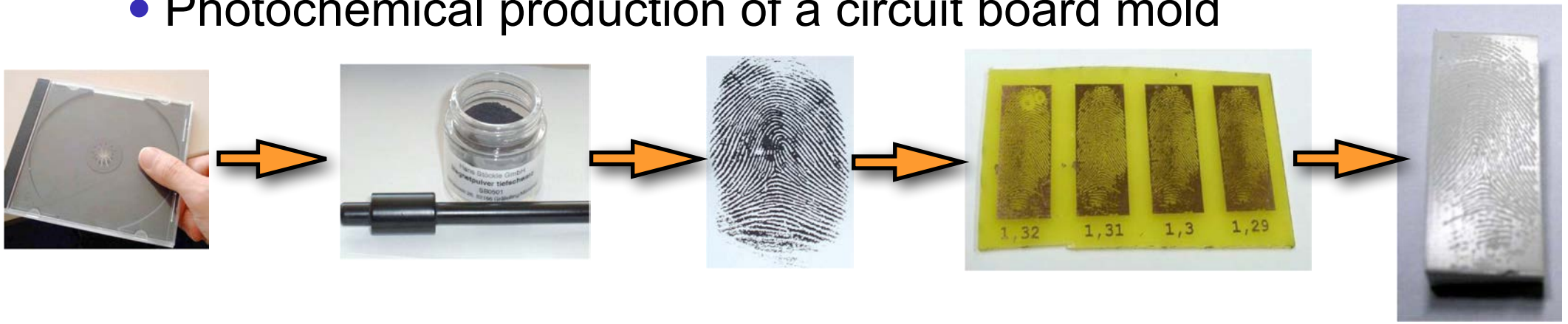
Security ?

- Presentation Attacks

Gummy Finger Production in 2000 !

Attack without support of an enroled individual

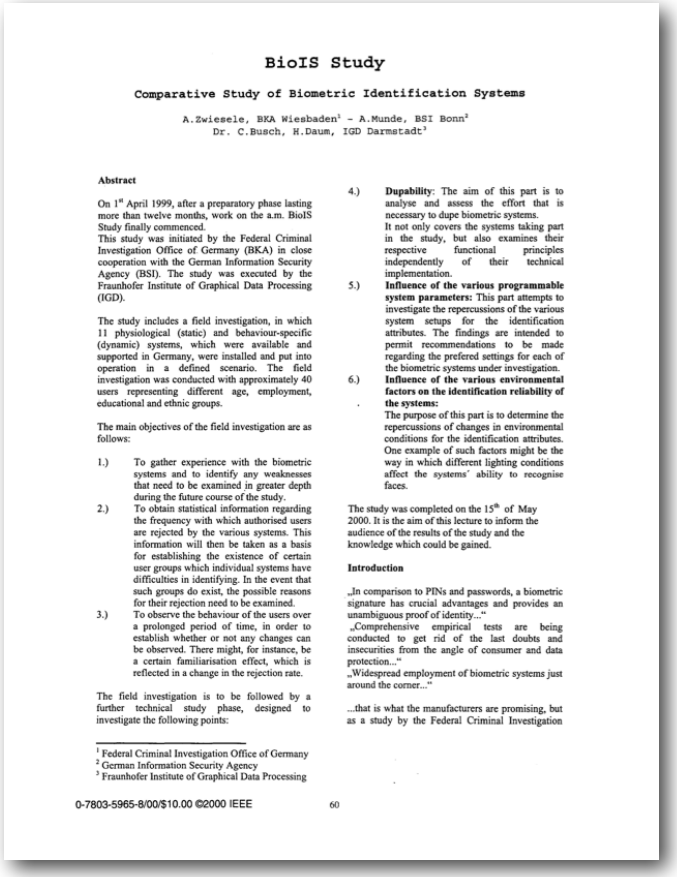
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board mold



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)



BioIS Study

Comparative Study of Biometric Identification Systems

A.Zwiesele, BKA Wiesbaden[1] - A.Munde, BSI Bonn[2]
Dr. C.Busch, H.Daum, IGD Darmstadt[3]

Abstract

On 1st April 1999, after a preparatory phase lasting more than twelve months, work on the a.m. BioIS Study finally commenced.
This study was initiated by the Federal Criminal Investigation Office of Germany (BKA) in close cooperation with the German Information Security Agency (BSI). The study was executed by the Fraunhofer Institute of Graphical Data Processing (IGD).

The study includes a field investigation, in which 11 physiological (static) and behaviour-specific (dynamic) systems, which were available and supported in Germany, were installed and put into operation in a defined scenario. The field investigation was conducted with appoximately 40 users representing different age, employment, educational and ethnic groups.

The main objectives of the field investigation are as follows:

1.) To gather experience with the biometric systems and to identify any weaknesses that need to be examined in greater depth during the future course of the study.
2.) To obtain statistical information regarding the frequency with which authorised users are rejected by the various systems. This information will then be taken as a basis for establishing the existence of certain user groups which individual systems have difficulties in identifying. In the event that such groups do exist, the possible reasons for their rejection need to be examined.
3.) To observe the behaviour of the users over a prolonged period of time, in order to establish whether or not any changes can be observed. There might, for instance, be a certain familiarisation effect, which is reflected in a change in the rejection rate.

The field investigation is to be followed by a further technical study phase, designed to investigate the following points:

4.) **Dupability**: The aim of this part is to analyse and assess the effort that is necessary to dupe biometric systems.
It not only covers the systems taking part in the study, but also examines their respective functional principles independently of their technical implementation.
5.) **Influence of the various programmable system parameters:** This part attempts to investigate the repercussions of the various system setups for the identification attributes. The findings are intended to permit recommendations to be made regarding the prefered settings for each of the biometric systems under investigation.
6.) **Influence of the various environmental factors on the identification reliability of the systems:**
The purpose of this part is to determine the repercussions of changes in environmental conditions for the identification attributes. One example of such factors might be the way in which different lighting conditions affect the systems' ability to recognise faces.

The study was completed on the 15th of May 2000. It is the aim of this lecture to inform the audience of the results of the study and the knowledge which could be gained.

Introduction

„In comparison to PINs and passwords, a biometric signature has crucial advantages and provides an unambiguous proof of identity..."
„Comprehensive empirical tests are being conducted to get rid of the last doubts and insecurities from the angle of consumer and data protection..."
„Widespread employment of biometric systems just around the corner..."

...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[1] Federal Criminal Investigation Office of Germany
[2] German Information Security Agency
[3] Fraunhofer Institute of Graphical Data Processing

0-7803-5965-8/00/$10.00 ©2000 IEEE

Presentation Attack Detection - Testing

Definition of harmonized metrics in ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as normal presentations at the component level in a specific scenario

- **Normal presentation classification error rate (NPCER)**
  proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario

Smartphone Access Control

Finger recognition study - 2012/2013

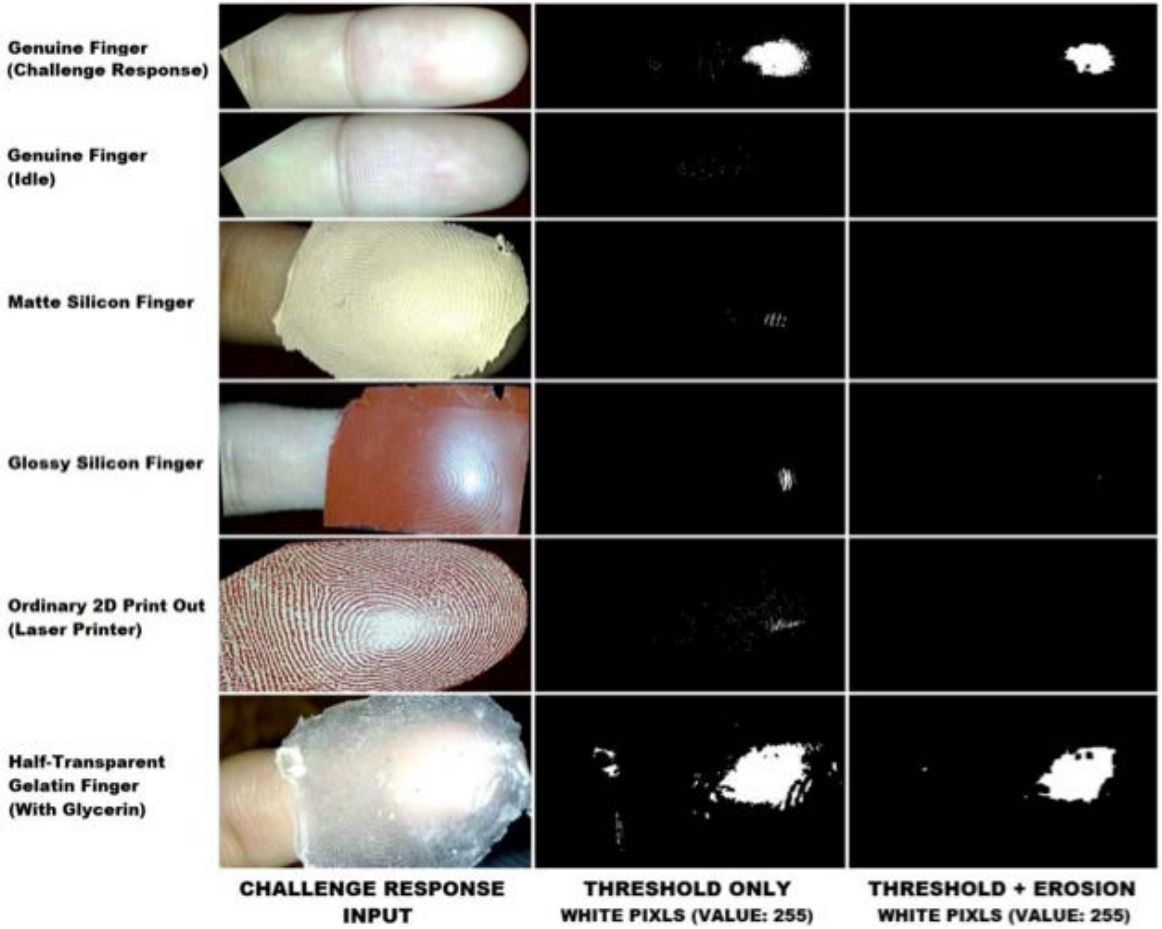
- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera
- Attack detection, as light reflection differs from artefacts to genuine fingers

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)



- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Smartphone Access Control - with PAD

Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information

Smartphone Access Control - with PAD

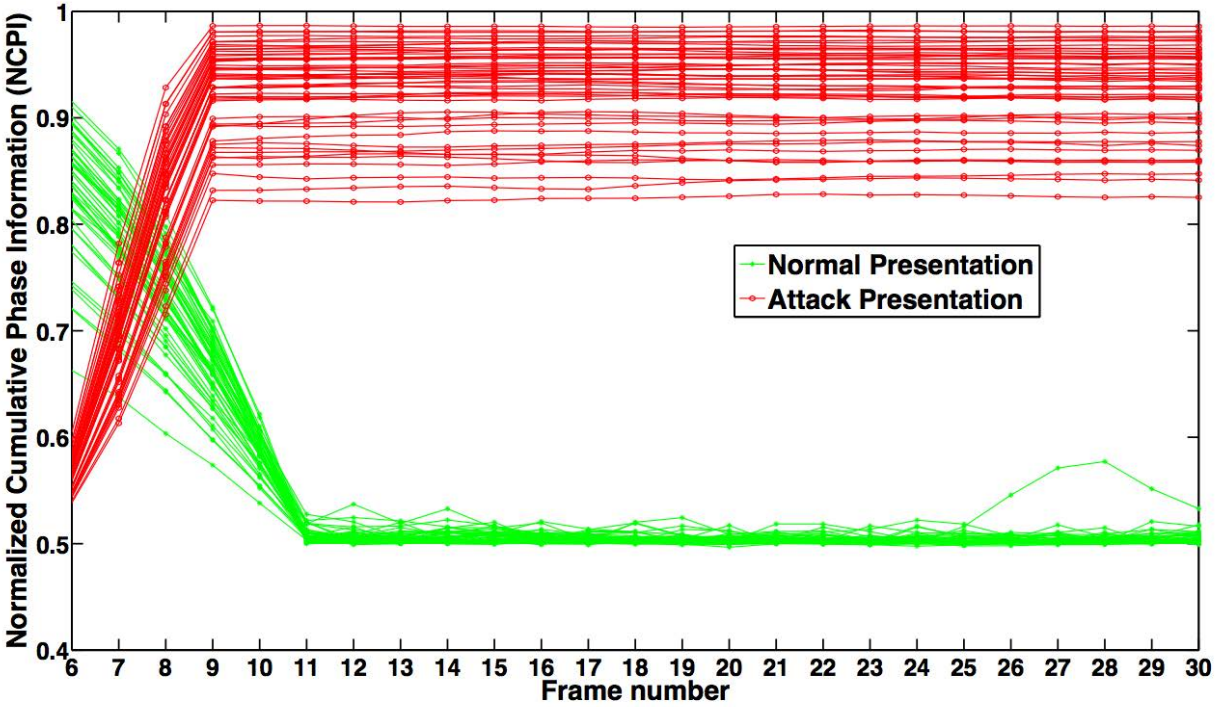
Method based on Eulerian Video Magnification (EVM)

[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Smartphone Access Control - with PAD

Eye recognition study - 2015

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information
- Zero Error Rates:
  - APCER = 0 %
  - NPCER = 0 %



[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Privacy Protection ?

Operators will think:

„Biometric systems must be compliant to data privacy and data protection principles“

Biometric Template Protection

We do NOT store fingerprint, iris or face images

- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Non-invertibility:Original biometric sample can not be reconstructed

- [Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008) http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf

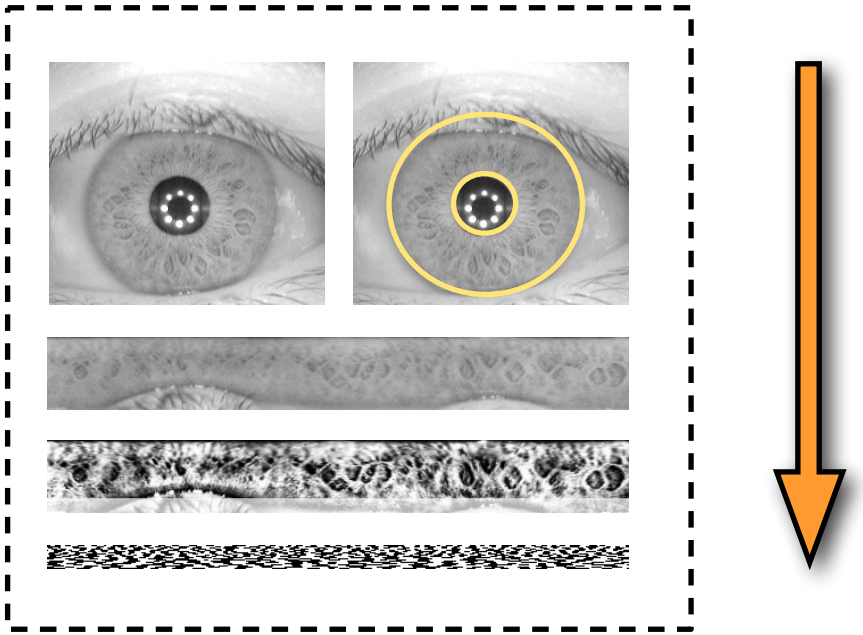
  [RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014) http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers
- Successfully applied to iris, face, fingerprint and fingervein

- Example: Iris Segmentation



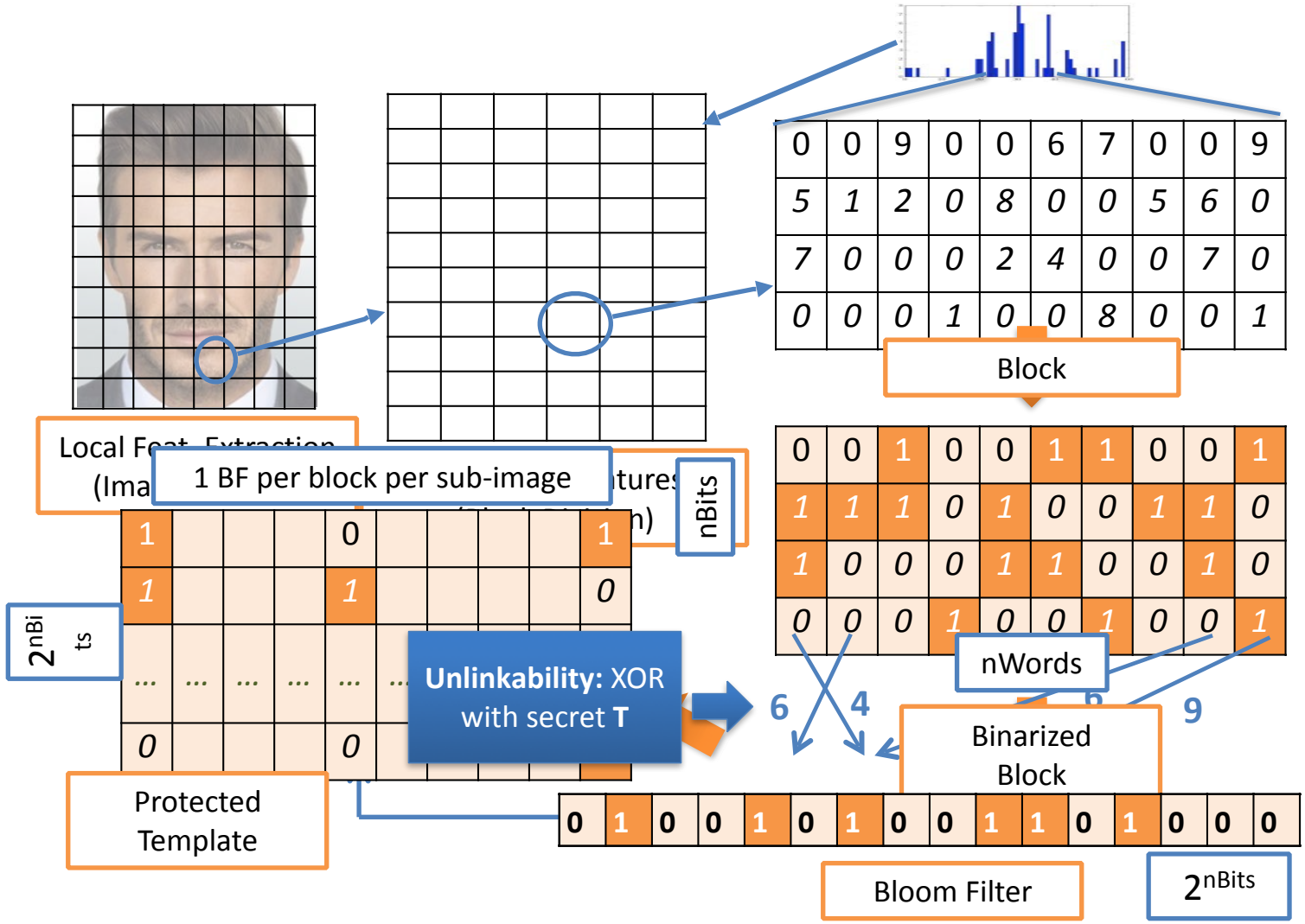
- Normalized Iris Texture
- Iris Feature Vector
- Binarised Iris Feature Vector

[Ra2014] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: „On the Application of Bloom Filters to Iris Biometrics“, in IET Journal on Biometrics 3(1), (2014)
http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Protection at the same accuracy level is possible

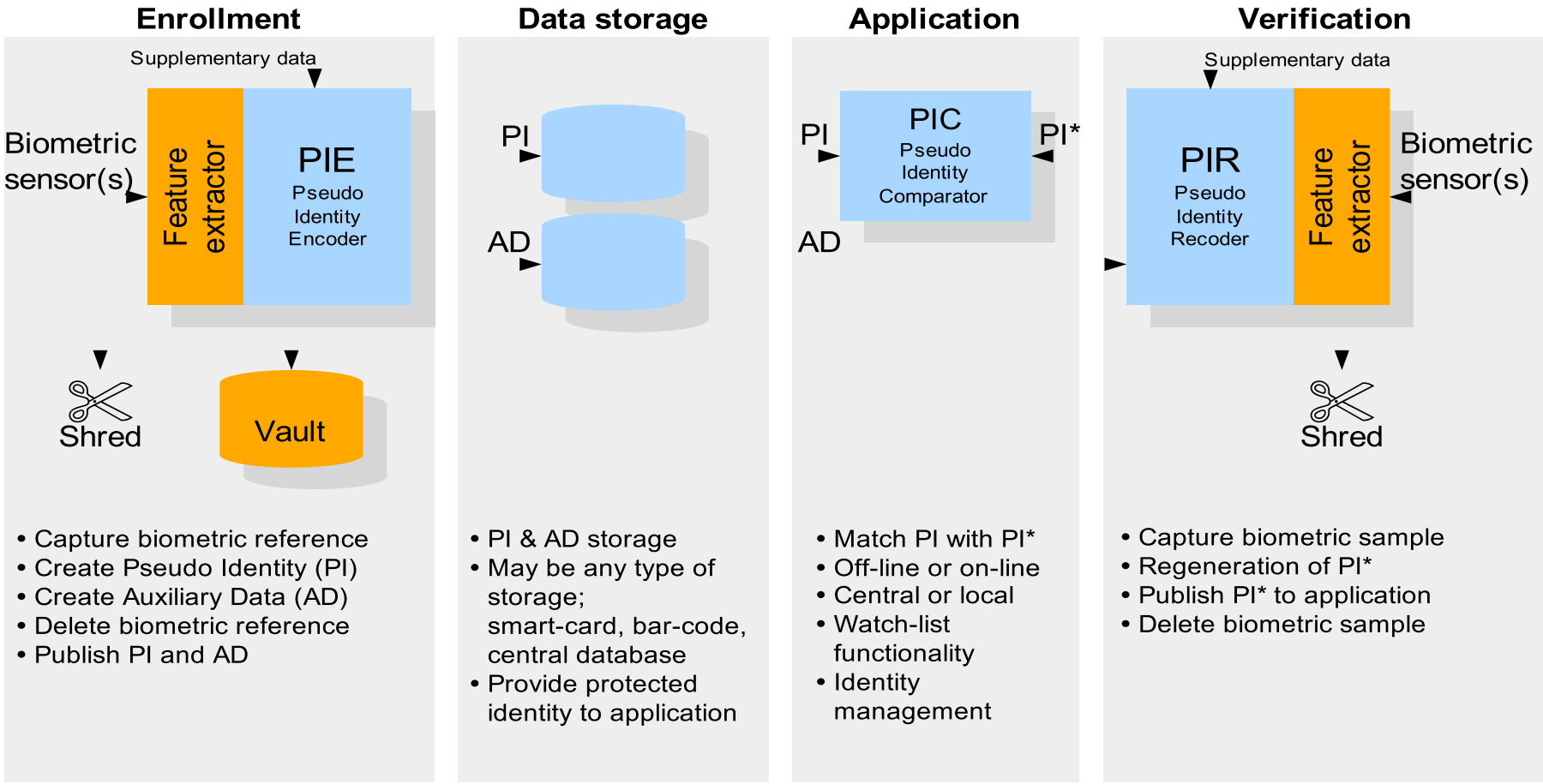
- Generating bloom filter-based pseudonymous identifiers



Data Protection Requirements

Technical framework on how to implement requirements for data privacy and data protection

- exists ISO/IEC 24745: Biometric Information Protection, (2011)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52946



Why multiple Modalities?

Financial Transactions

- Position of the Bundesverband Deutscher Banken (BdB)
  - number and strength of biometric factors should scale with transaction volume

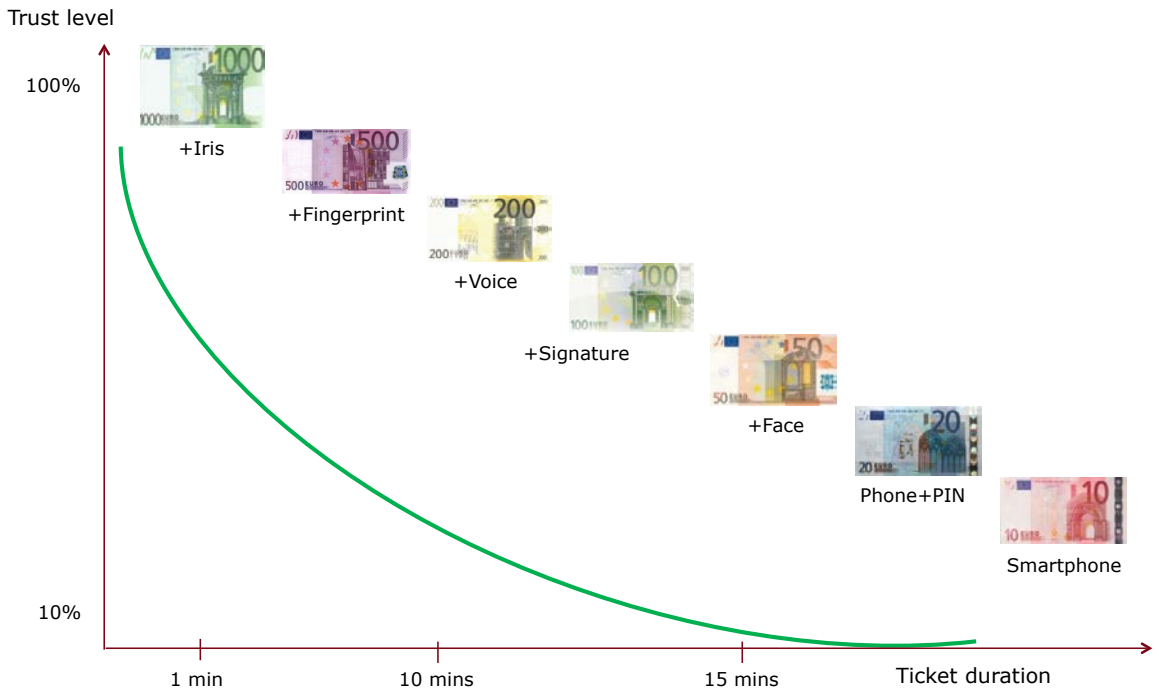


Image Source: BdB 2015

[Gru2015] W. Grudzien, „Current trends in the payments and transactions landscape" Bundesverband Deutscher Banken, October 2015

Mobile Biometric Payment - Biometric Transaction and Authentication Protocol (BTAP)

Biometric Transaction Authentication Protocol

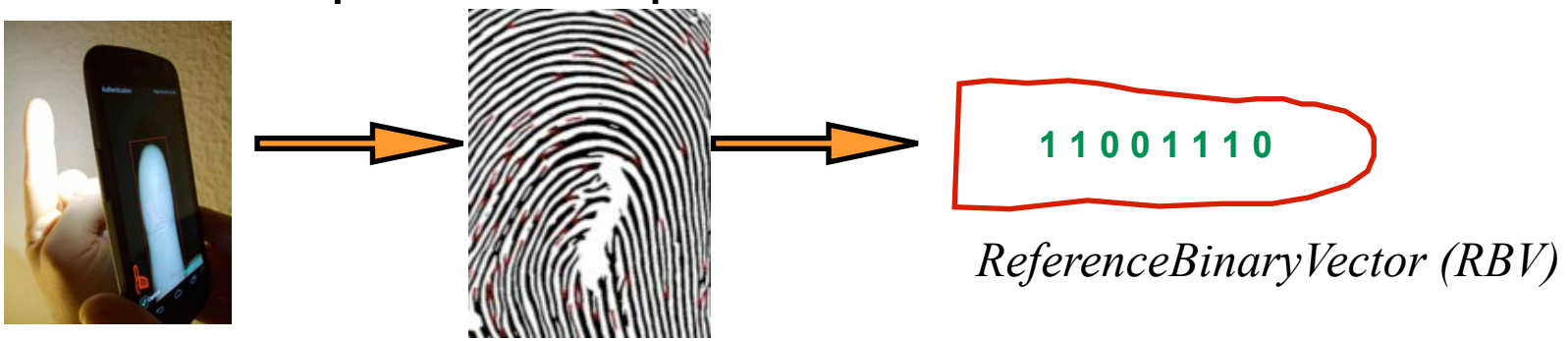
Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret

- received via subscribed letter from the bank
- entered once to the smartphone
  - hash over the secret constitutes a Pseudonymous Identifier

2.) Biometric enrolment

- Biometric samples are captured

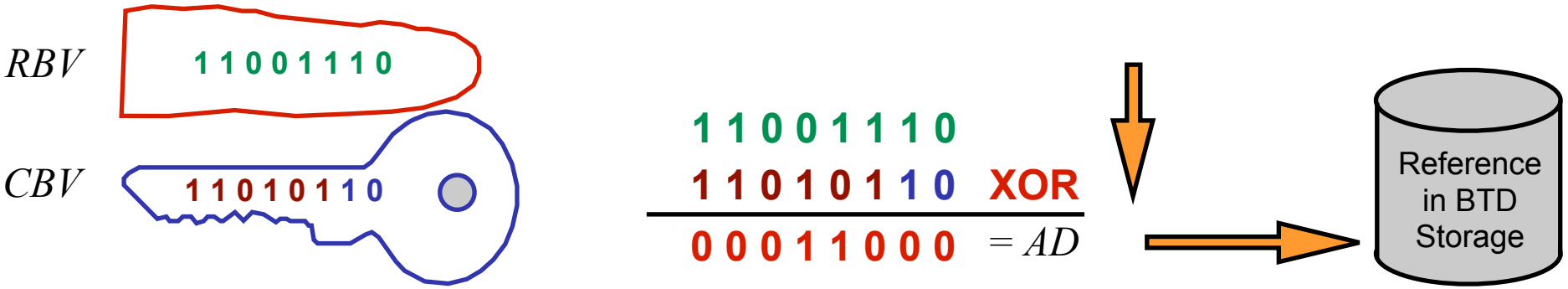


Biometric Transaction Authentication Protocol

Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of auxilliary data

- we neither store the confidential secret nor the sensitive biometric data (i.e. feature vector)
- the secret and biometric data are merged



- Auxilliary data (AD) stored in the Smartphone
  - Biometric Transaction Device = FIDO Authenticator

Transaction-Verification

BTAP-Video

- http://christoph-busch.de/files/BTAP.mp4

Conclusion

Biometrics is possible with todays smartphones

- a multi-biometric authentication scheme with scaling factors is a good choice with respect to security threats

Biometric standards are available

- financial transaction schemes should follow technical standards
- financial transaction schemes should follow privacy standards

BTAP follows the two channel concept

- is based on international ISO/IEC standards
- is privacy friendly as no biometric reference is stored on a banking server

More and detailed information on BTAP at:

http://www.christoph-busch.de/projects-btap.html

Contact

Contact: